

Lab 2: Network Analyzer - Wireshark

Lab Objective:

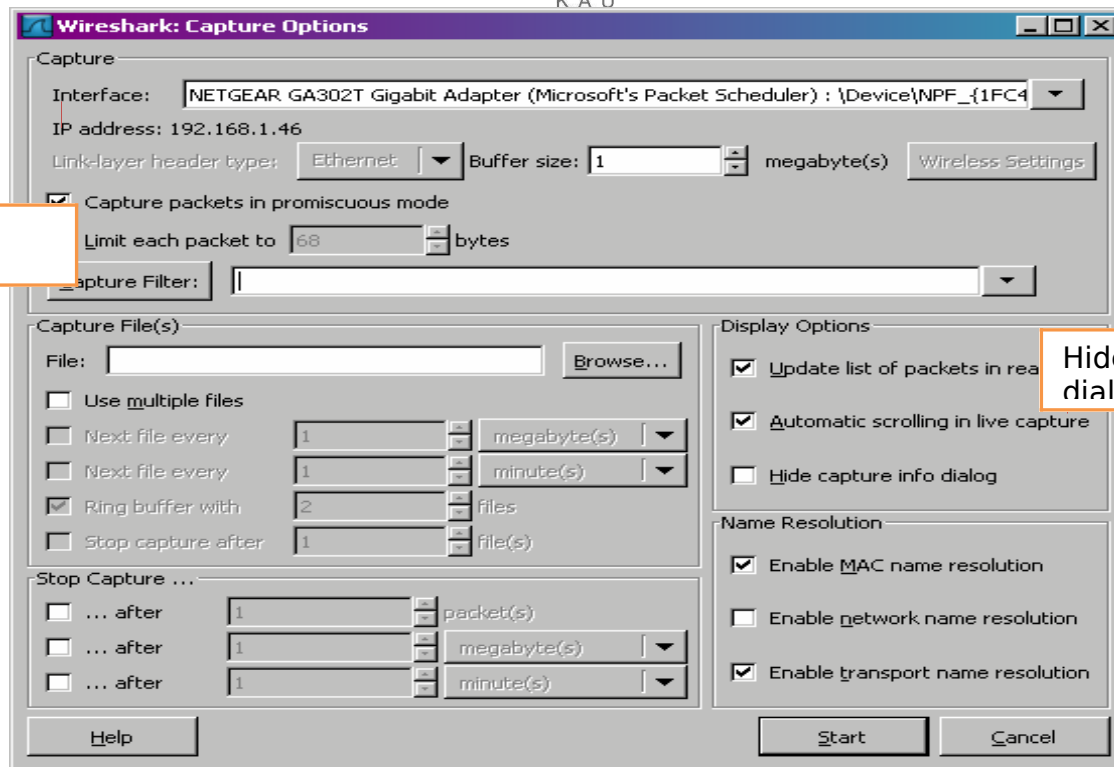
- To introduce “wireshark” with the basic **utilities/tools** of data communication and networking.

Introduction:

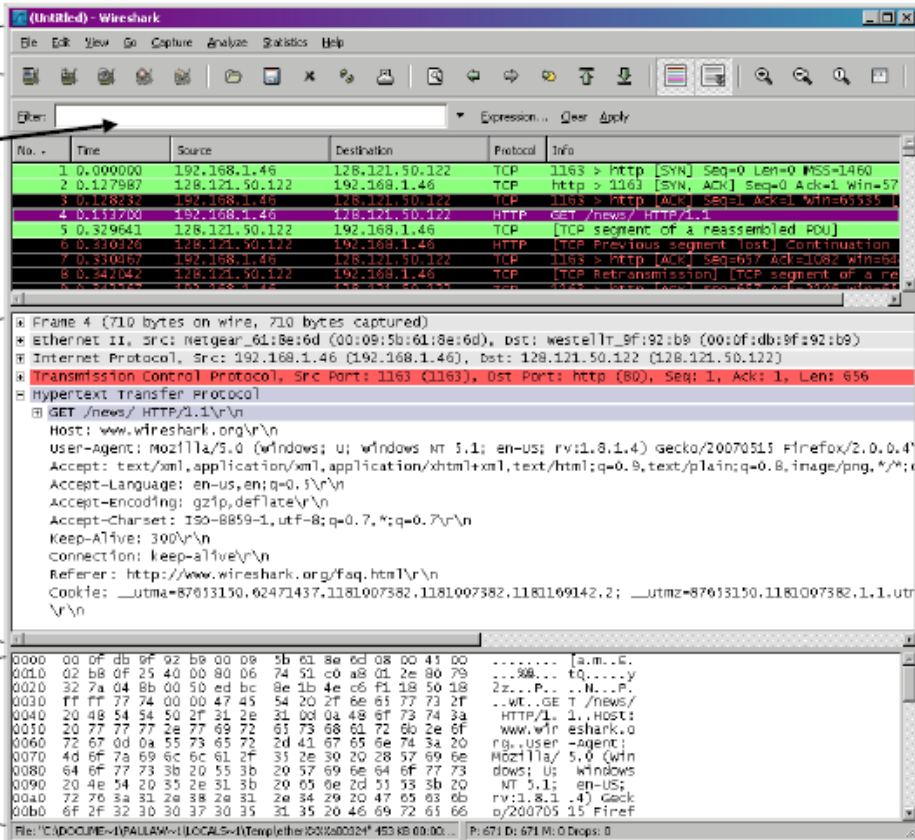
- Wireshark is the world's most popular network analyzer.
- It is a very powerful tool that provides network and upper layer protocols information about data captured in a network.
- The Wireshark strength comes from:
 - ◊ Its easiness to install.
 - ◊ The simplicity of use of its GUI interface.
 - ◊ The very high number of functionality available.

Activities:

1. Run Wireshark
2. Configure Wireshark for your NIC and select the interface that you will be using
Capture → Interfaces OR Capture → Options



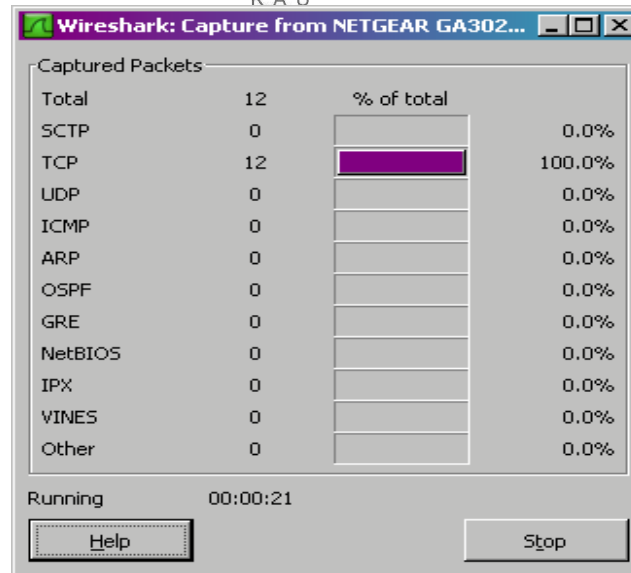
3. Configure the properties of your chosen capture interface
4. Start and begin your first trace in real time network.



The image shows the Wireshark network protocol analyzer interface. It is divided into several panes:

- command menus:** The top menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Help) and the toolbar below it.
- display filter specification:** The filter bar below the toolbar, currently showing an empty filter.
- listing of captured packets:** The packet list pane on the left, showing a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info.
- details of selected packet header:** The packet details pane on the right, showing the hierarchical structure of the selected packet (Frame 4). The selected packet is a GET request from 192.168.1.46 to 128.121.50.122.
- packet content in hexadecimal and ASCII:** The packet bytes pane at the bottom, showing the raw data of the selected packet in hexadecimal and ASCII.

5. Uncheck the "Hide capture info dialog" option in the Capture Options dialog box
6. View packets that you have captured in packet list pane, which will bring up the selected packet in the tree view and byte view panes.



7. Use the wireshark user guide from help.
8. Go to the chapter 3: User Interface and explore all the menu options

Questions:

1. What did you understand from "Hide Capture Info dialog" option?
2. How can we filter out the packets while capturing packets?
3. If you do not check the option "Capture packets in promiscuous mode" in the capture option dialog. Does wireshark would be able to capture all the packets on this network segment? State the reason.
4. What did you understand from "capture filter" and "display filter" dialog box?
5. How can you find a specific packet by knowing packet number?
6. Write down the purpose of using wireshark? What are the possible pros and cons of using it?

Lab Assignment:

1. How to specify a capture filter for telnet that captures traffic to and from a particular host (IP)

2. How to filter out packet list pane down to only those packets to or from your computer IP using display filter.
3. How to filter out packet list pane to all the packets excluding your computer IP using display filter.
4. Test run and capture the network activity between the FTP server and its client (hint: while Wireshark is running, open your browser and enter the FTP server. Capture *username* and *password* entered by user through wireshark).

Hint:

5. Filtering while capturing (section 4.9)
6. Filtering packets while viewing (section 6.3)
7. Defining and saving filters (section 6.6)